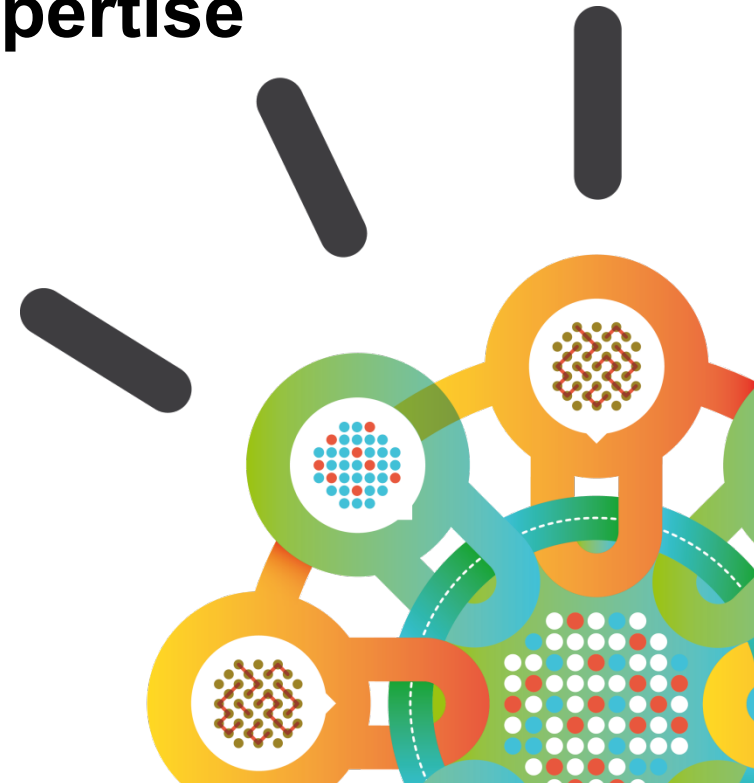


Security Intelligence.  
Think Integrated.

# IBM Security

## Intelligence, Integration and Expertise

IBM Security Systems  
November 2013





## Agenda

- Welcome and Introductions
- Latest Security trends and H1 2013 X-Force Report
- Security Intelligence - Understanding your Organizational Security Posture
- Holistic approach to handling Advanced Persistent Threats
- Break
- **From Identity & Access Management to Identity Intelligence**
- Managing Application Security
- Data Security

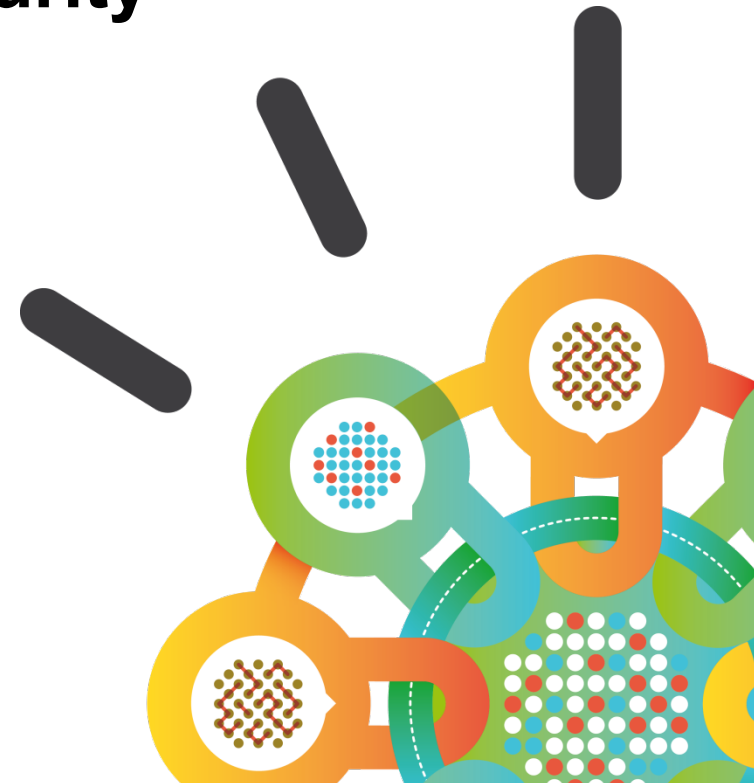


## Agenda

- Welcome and Introductions
- Latest Security trends and H1 2013 X-Force Report
- Security Intelligence - Understanding your Organizational Security Posture
- Holistic approach to handling Advanced Persistent Threats
- Break
- From Identity & Access Management to Identity Intelligence
- **Managing Application Security**
- Data Security

Security Intelligence.  
**Think Integrated.**

# IBM Security – Application Security





# Solving Customer Challenges

## *Application Security*



### **Finding the vulnerabilities**

Leverage advanced and extensive testing methodologies



### **Building products that are secure by design**

Reduce costs by integrating security testing early in the development lifecycle



### **Bridging the Security/Development gap**

Engaging Security and Development organizations to collaboratively address application vulnerabilities



### **Controlling access to application data**

Strengthen applications and data access on a need to know basis



# Solving Customer Solutions

## Application Security



### Finding Application Vulnerabilities

*“GlassBox scanning allowed us to improve results accuracy as well as test for new class of vulnerabilities undetected by conventional web application security scanning technologies”*

*Boris Gorin, Amdocs*



### Reducing the Cost of Being Secure

*“AppScan not only helps us to avoid costs related to hacking attacks, but also reduces the manual effort needed for analysis and the costs for testing”*

*Michael Neumaier, Senior Quality Specialist, SAP AG*



### Providing Oversight and Governance

*“We were able to increase the participation of the IT community in web application scanning”*

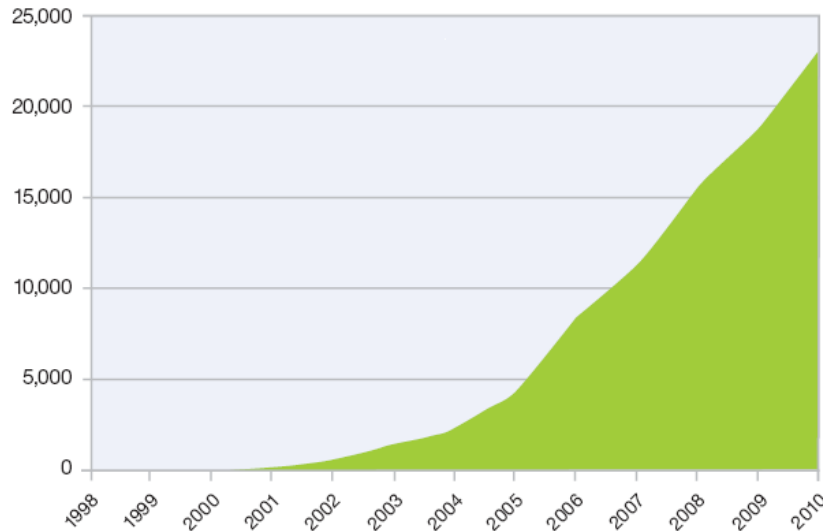
*Alex Jalso, Assistant Director, Office of Information Security, WVU*



# The Application Security landscape

## Web application vulnerabilities dominate the enterprise threat landscape

Cumulative Count of Web Application Vulnerability Disclosures  
1998-2010



- 37% of all new vulnerabilities are in web applications (2011 1H)\*
- ~4K new application vulnerabilities reported every year from 2006-2010\*\*

### Applications in Development

- In-house development
- Outsourced development

### Production Applications

- Developed in house
  - Acquired
  - Off-the-shelf commercial apps
- Vulnerabilities are spread through a wide variety of applications

# Adopt a *Secure by Design* approach to enable you to design, deliver and manage smarter software and services

- Build security into your application development process
- Efficiently and effectively address security defects **before deployment**
- Collaborate effectively between Security and Development
- Provide Management visibility



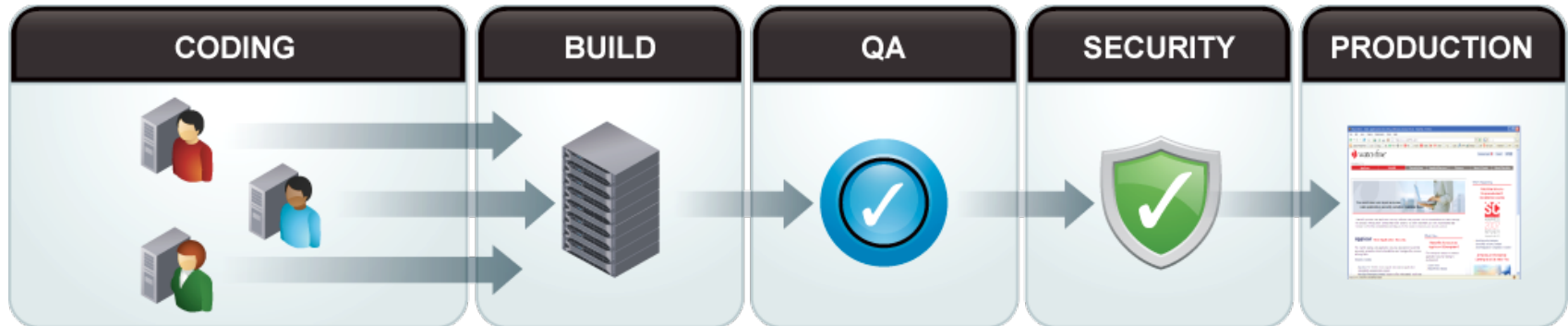
Deliver New Services Faster



Innovate Securely



Reduce Costs

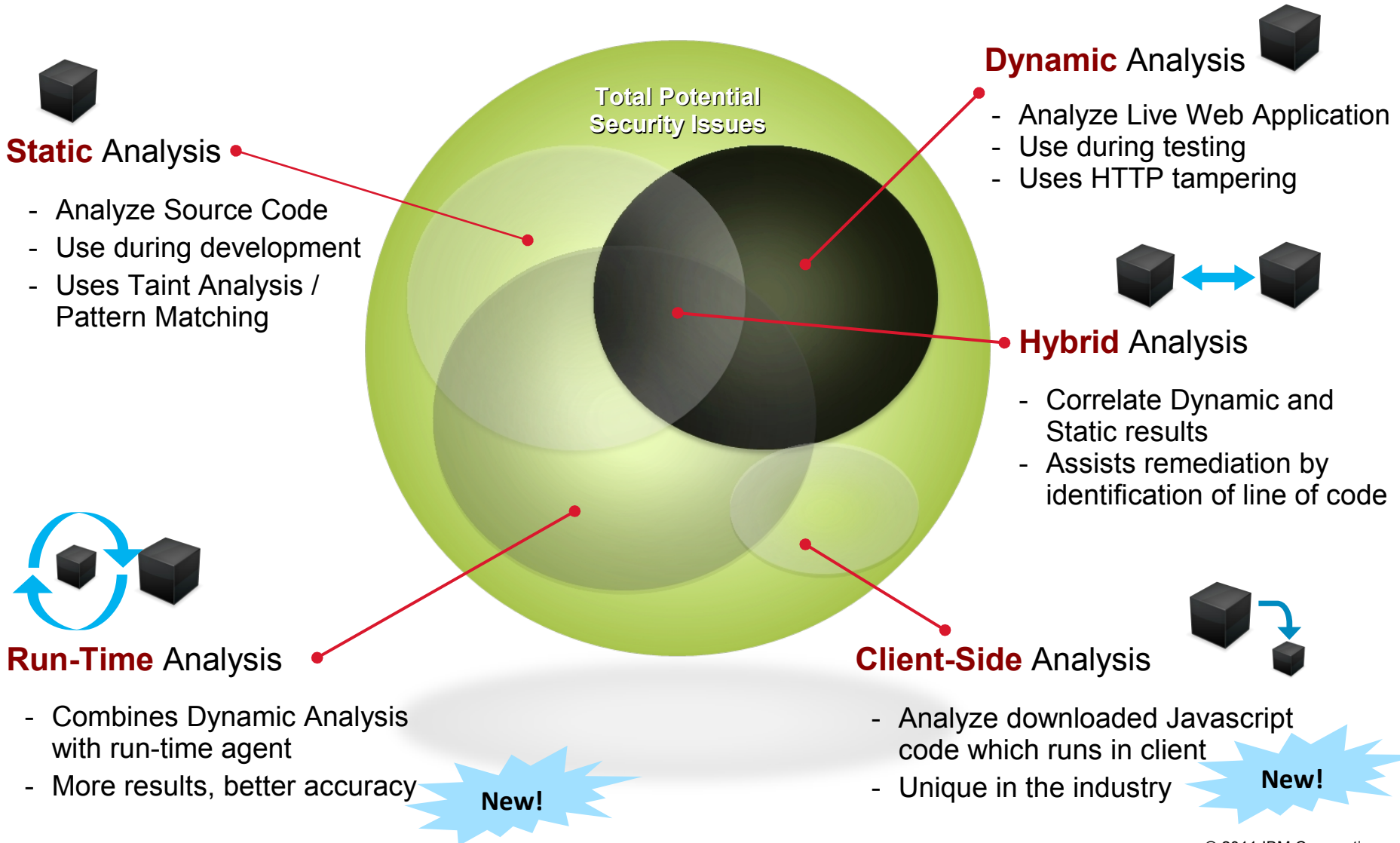


**Proactively address vulnerabilities early in the development process**





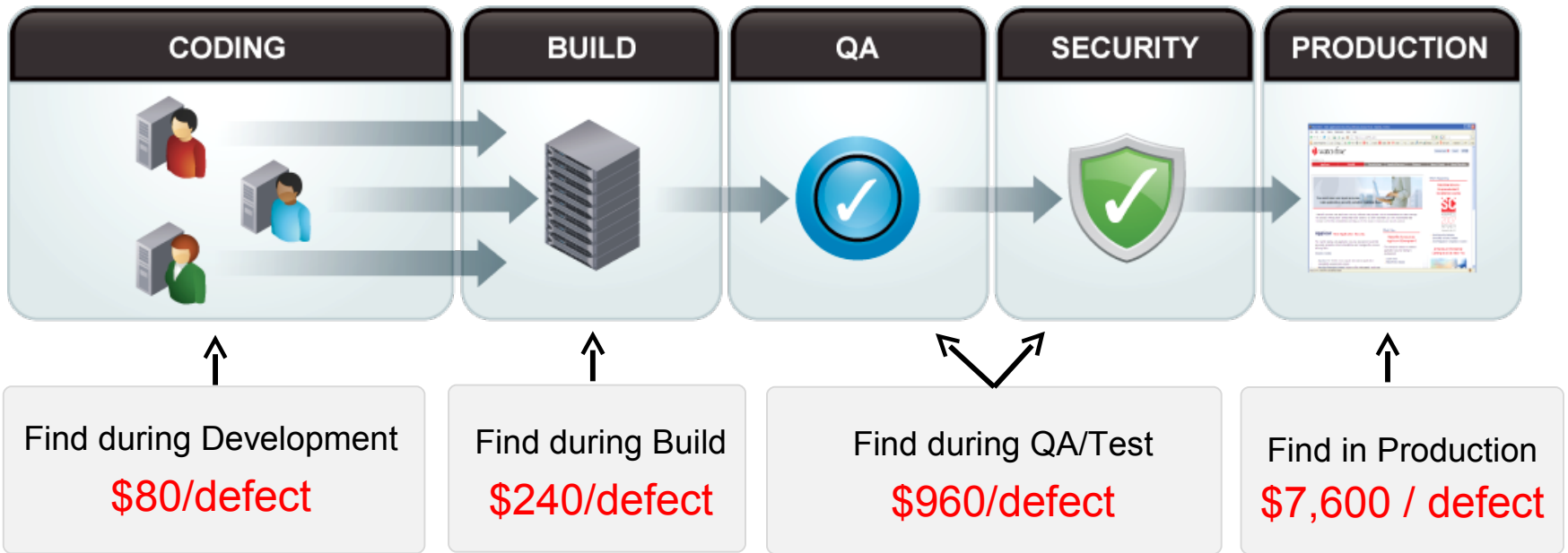
# Challenge 1: Finding more vulnerabilities using advanced techniques



# Challenge 2: Reducing Costs Through a Secure by Design Approach

80% of development costs are spent identifying and correcting defects!\*

Average Cost of a Data Breach \$7.2M\*\* from law suits, loss of customer trust, damage to brand



*“As financially-motivated attackers have shifted their focus to applications, Web application security has become a top priority. However, the responsibility for web application security cannot rest solely with information security. Enterprises should evaluate how to identify vulnerabilities in Web applications earlier in the development process as transparently as possible using web application security testing products or services.”*  
 Neil MacDonald, Gartner, 12-6-11

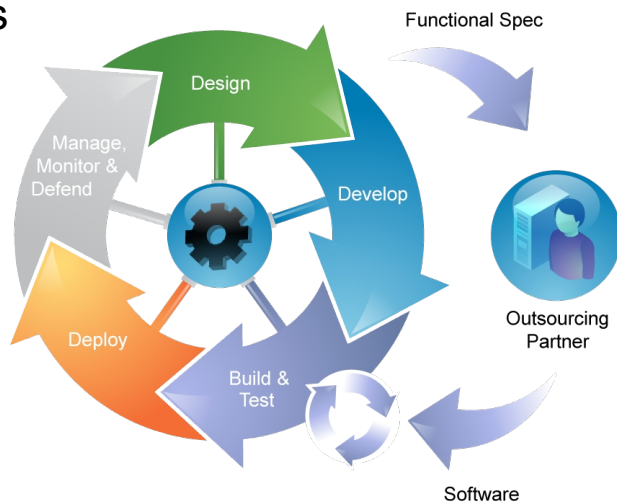
\* Source: National Institute of Standards and Technology

\*\* Source: Ponemon Institute 2009-10

# Challenge 3: Bridging the Security/Development gap

## Break down organizational silos

- Security experts establish security testing policies
- Development teams test early in the cycle
- Treat vulnerabilities as development defects



## Provide Management Visibility

- Dashboard of application risk
- Enable compliance with regulation-specific reporting



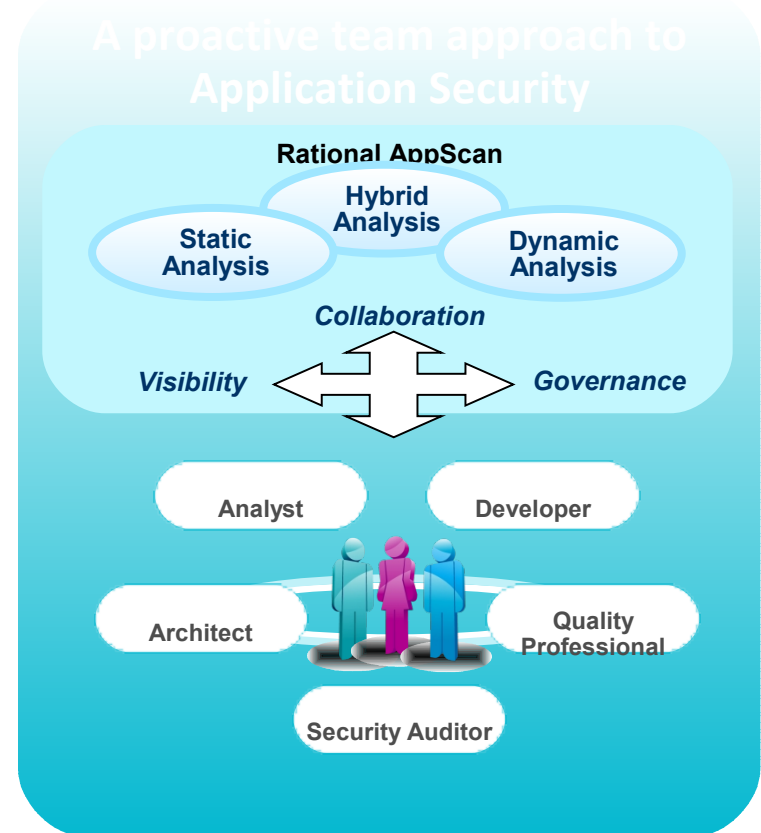
“... we wanted to go to a multiuser web-based solution that enabled us to do concurrent scans and provide our customers with a web-based portal for accessing and sharing information on identified issues.”

Alex Jalso, Asst Dir, Office of InfoSecurity, WVU



## Organizations need to take a *proactive approach* to Application Security

- **Embed security testing early** in the development lifecycle to support agile delivery demands
- Bridge the gap between “Security” and “Development” through **joint collaboration and visibility**, enabling regulatory compliance
- Integrate security testing **into the development lifecycle**, through interfaces to development tools





# Challenge 4: Controlling Access to Data

## IBM Security Policy Manager

Manage and enforce fine-grained entitlement and message security policy management

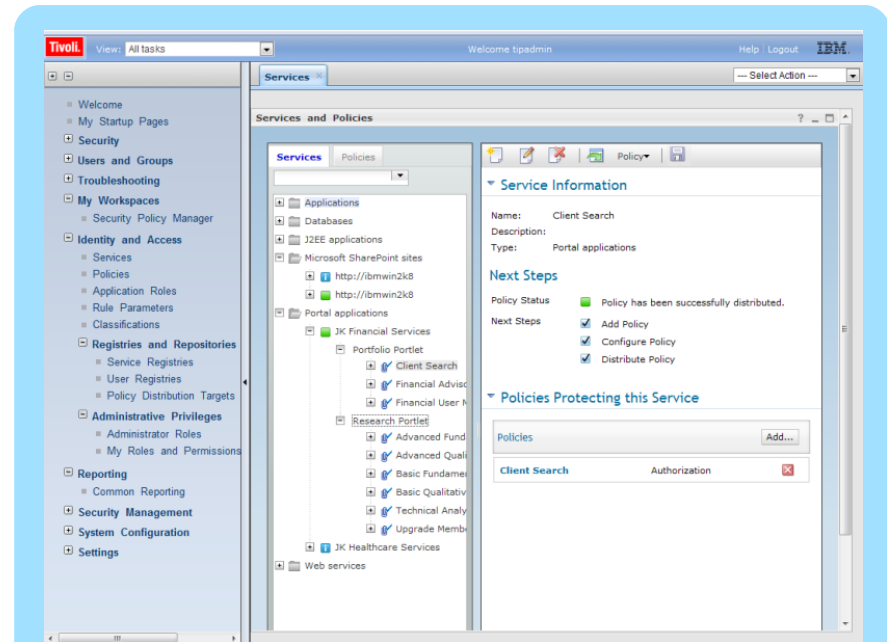
### Strengthen application security and data access on a need to know basis

#### Business Challenge

Protect fine-grained access to data for business critical applications, databases, portals and services

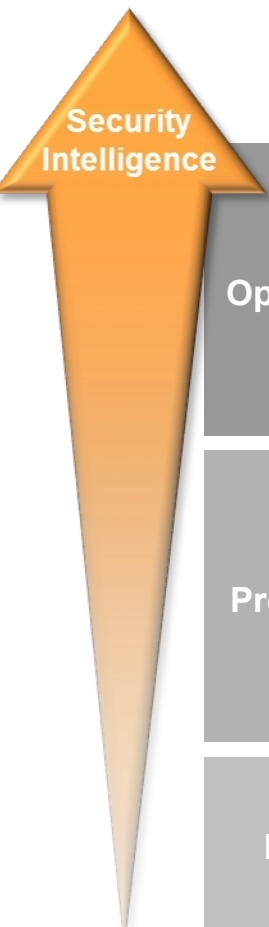
#### Key solution highlights

- Improved time to value for DataPower deployments with central policy management
- Enforce entitlement policy across application middleware, portals and databases
- Improved scalability for large number of services and policies
- Centralized security policy authoring and distributed enforcement



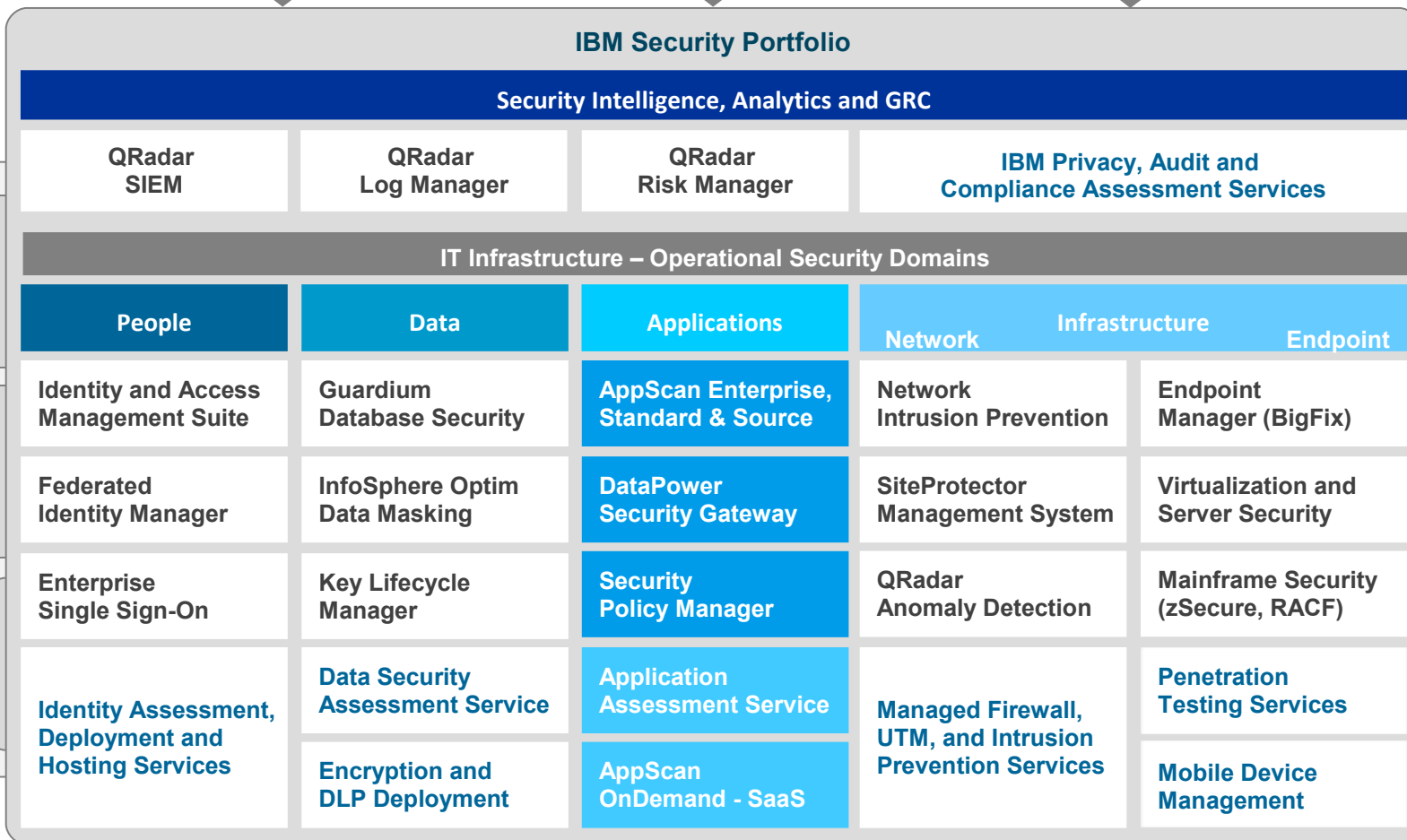
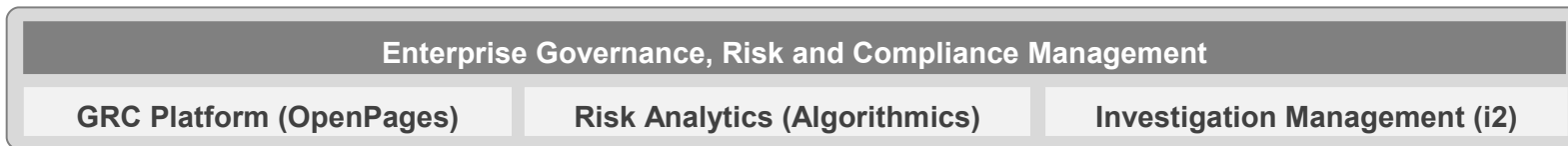
**Reduce cost and risk of implementing applications security to address compliance**

# Helping Organizations Progress in Their Security Maturity



	People	Data	Applications	Infrastructure	Security Intelligence
Optimized	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	<b>Secure app engineering processes</b> <b>Fraud detection</b>	Advanced network monitoring Forensics / data mining Securing systems	Advanced threat detection Network anomaly detection Predictive risk management
Proficient	User provisioning Access mgmt Strong authentication	Access monitoring Data loss prevention	<b>Application firewall</b> <b>Source code scanning</b>	Virtualization security Asset mgmt Endpoint / network security management	Real-time event correlation Network forensics
Basic	Centralized directory	Encryption Access control	<b>Application scanning</b>	Perimeter security Anti-virus	Log management Compliance reporting

# IBM's security product and service portfolio...



Security Consulting

Managed Services

X-Force and IBM Research

v12-04

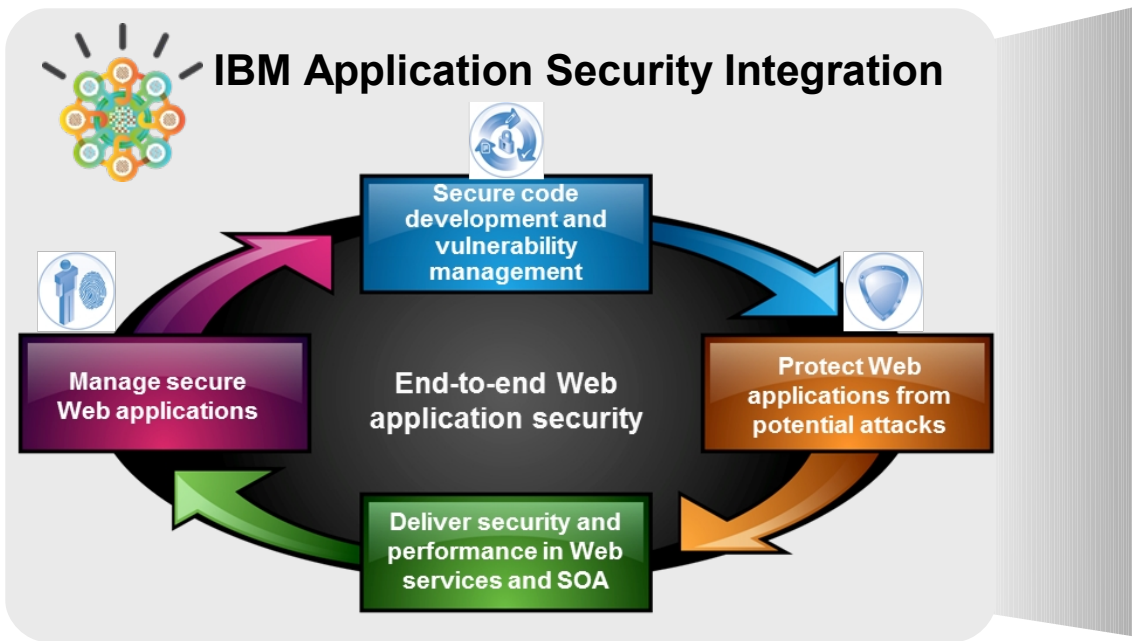
Products    Services

Application Security Products

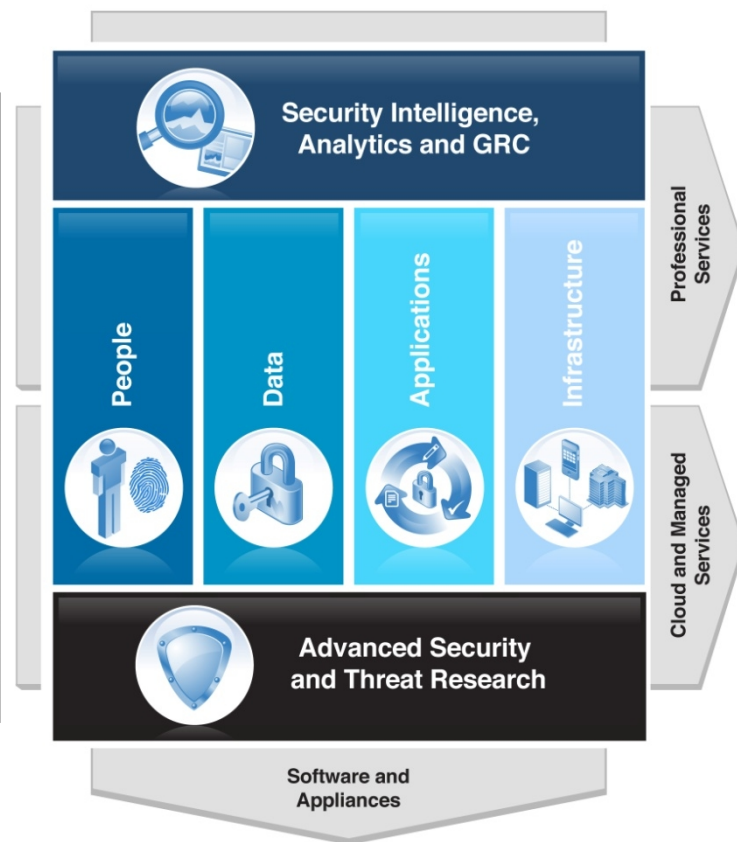
Application Security Services

# Application Security. Think Integrated

*Integrate secure development, vulnerability management, network and host protection*



### IBM Security Framework





## Why IBM Security: Breadth, deep expertise, integration

### Leadership

- “After doing our research, we determined that IBM was a leader in the field of dynamic application scanning.”  
*Alex Jalso, Assistant Director, Office of Information Security, WVU*
- Identified as a Leader in Gartner SAST Magic Quadrant, December 2010
- Identified as a Leader in Gartner DAST Magic Quadrant, December 2011
- Pioneer of new hybrid analysis techniques, including Correlation, JavaScript Analyzer and GlassBox
- Pioneer of developer-friendly solutions

### Integration

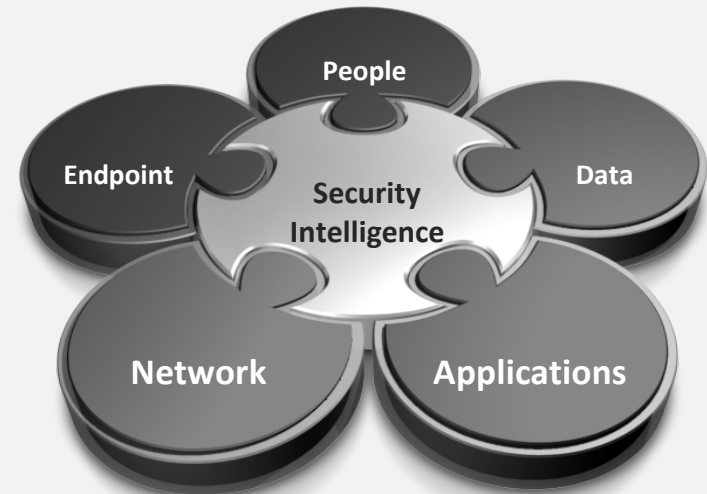
- Integration with IBM AppScan and SiteProtector to enhance web through IPS policy modification from
- Integrates with IBM Rational development lifecycle solutions to collaboration between security and development teams

### Expertise

- “We turned to IBM because they offered both the technology leadership and the deep security expertise...”  
*Marek Hlávka, Chief Security Officer, Skoda Auto*

## Think Integrated.

enable



[ibm.com/security](http://ibm.com/security)



© Copyright IBM Corporation 2012. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.



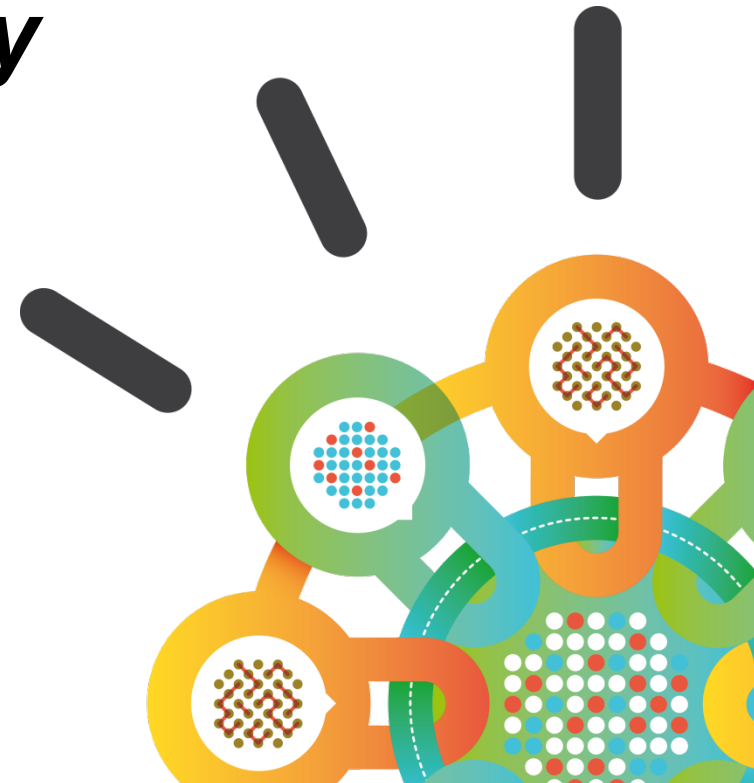
## Agenda

- Welcome and Introductions
- Latest Security trends and H1 2013 X-Force Report
- Security Intelligence - Understanding your Organizational Security Posture
- Holistic approach to handling Advanced Persistent Threats
- Break
- From Identity & Access Management to Identity Intelligence
- Managing Application Security
- **Data Security**

Security Intelligence.  
Think Integrated.

# ***Data Security: The Compliance Journey***

*Jakes Vorster*  
*Client Technical Professional*



## Agenda

- The Scary Reality of Data Security
- What is Guardium?
- PCI-DSS
- PoPI
- The Industry Leader
- Our Existing Customer Base
- Questions?

• ANDRE MAGINOT

3066-4



41317A

Andre Maginot

# Perimeter Defenses & Identity Management No Longer Sufficient

**“A fortress mentality will not work in cyber. We cannot retreat behind a Maginot Line of firewalls.”** William J. Lynn III, U.S. Deputy Defense Secretary

49% of new vulnerabilities are **Web application vulnerabilities**  
(X-Force)

**SQL Injection** is a leading attack vector  
(X-Force)

Kneber Botnet **stole 68,000 credentials & 2,000 SSL certificates** over 4-week period  
(NetWitness)

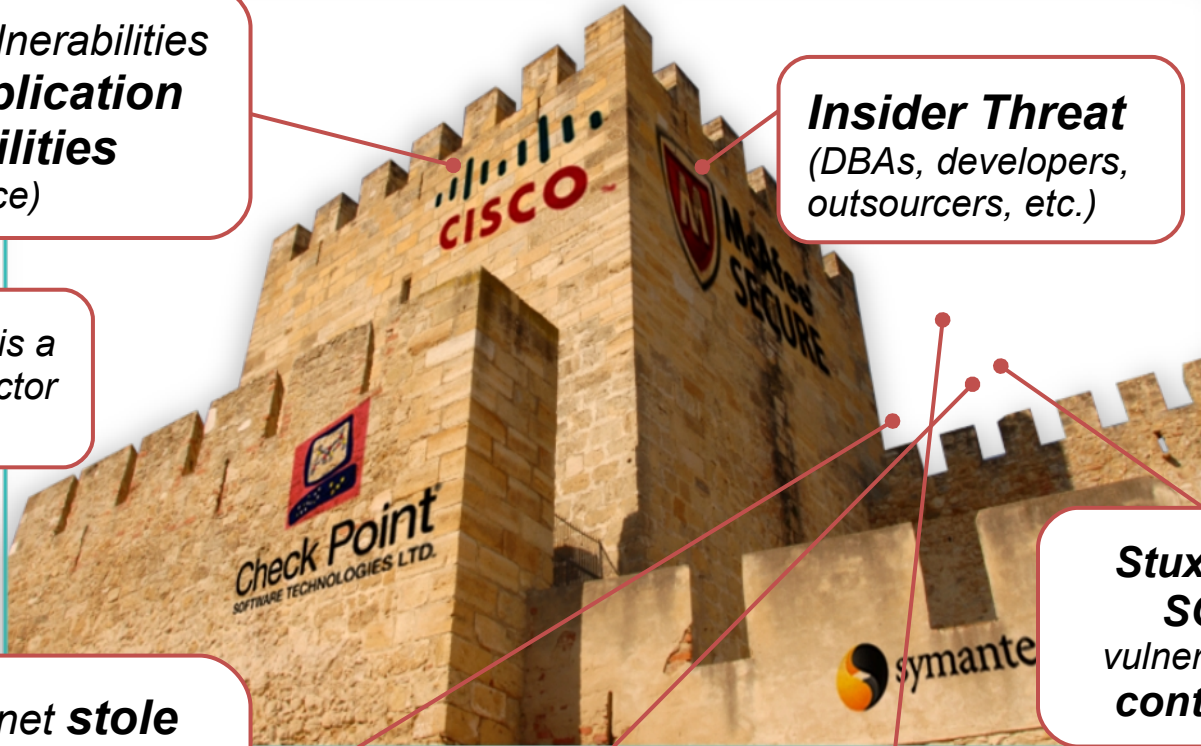
**Epsilon data breach affects millions**  
(outsourced provider)

**Insider Threat**  
(DBAs, developers, outsourcers, etc.)

**88% of F500 companies** have **employees infected with ZeuS**  
(RSA)

**Stuxnet exploited SQL Server vulnerability** to attack **control systems**

**#1 VM vulnerability is VM guest hopping**  
(hypervisor escape) (X-Force)



# The findings

**37%** of breaches affected financial organizations (+)

**14%** committed by insiders (+)

**13%** resulted from privilege misuse and abuse

**54%** compromised servers (-)

**69%** discovered by external parties

**66%** took months or more to discover (+)





## Cybercrime is a national crisis

Cybercrime has become a national crisis, said South African Centre for Information Security CEO **Beza Belayneh** on Tuesday, equating the scale to that of South Africa's prevalent HIV/Aids pandemic.



Cybercrime a 'national crisis', data breach risk grows

"Governments are hacked, police websites are hacked, banks are losing millions – the statistics are that South Africa loses R1-billion a year, and it now threatens human life," he said.

State Security Minister **Siyabonga Cwele** affirmed that the nation, along with the rest of the world, was "vulnerable" to cybercrime, and that the government was progressing a cybercrime policy aimed at mitigating the challenge.

## What most enterprises are doing today

### Rely on native audit logs within DBMS

#### ×Lack visibility and granularity

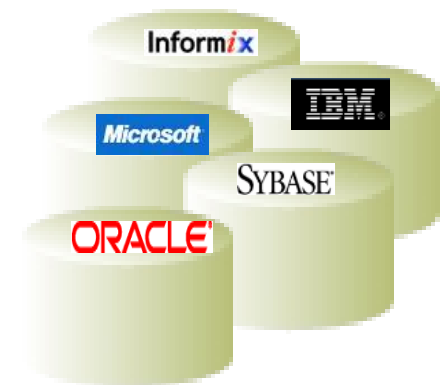
- Privileged users difficult to monitor
- Tracing the “real user” of application is difficult
- Level of audit detail is insufficient

#### ×Inefficient and costly

- Impact database performance
- Manual reporting, alerting and forensics
- Different methods for each DB type

#### ×No segregation of duties

- DBAs manage monitoring system
- Privileged users can bypass the system
- Audit trail is unsecured



## Key Business Drivers for Database Activity Monitoring (DAM)

### 1. Prevent data breaches

- Cybercriminals & rogue insiders
- Protect customer data & corporate secrets (IP)



### 2. Assure data governance

- Prevent unauthorized changes to sensitive data by privileged users

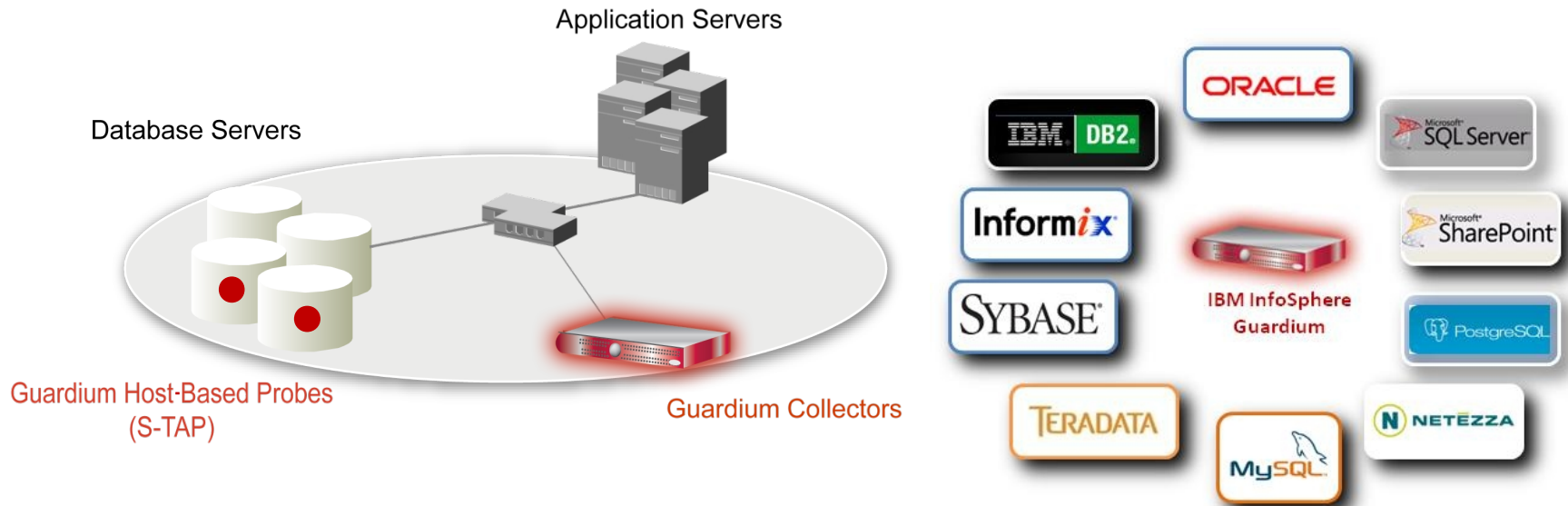


### 3. Reduce audit costs

- Automated, continuous controls
- Simplified processes



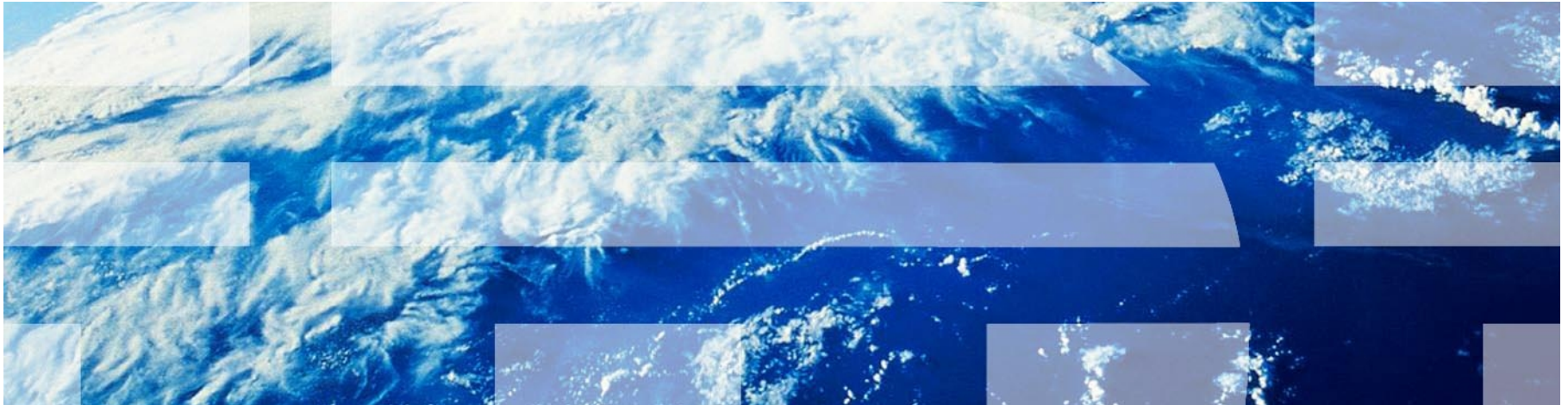
# Non-Invasive, Real-Time Database Security & Monitoring



- Continuously monitors all database activities (including local access by superusers)
- Heterogeneous, cross-DBMS solution
- Does not rely on native DBMS logs
- Minimal performance impact
- No DBMS or application changes
- Supports Separation of Duties
- Activity logs can't be erased by attackers or DBAs
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)
- Granular, real-time policies & auditing
  - *Who, what, when, where, how*

# Payment Card Industry Data Security Standard

# *PCI-DSS*



## What is PCI DSS?

The Payment Card Industry Security Standards Council is an open global forum for the ongoing **development, enhancement, storage, dissemination & implementation of security standards.**

The PCI Security Standards Council developed the **Payment Card Industry Data Security Standard (PCI DSS)** for account data which is: cardholder data + sensitive authentication data.

**PCI DSS applies to wherever account data is stored, processed or transmitted.**

<b>Cardholder data includes:</b>	<b>Sensitive authentication data includes:</b>
▪ Primary account number (PAN)	▪ Full magnetic stripe data
▪ Cardholder name	▪ CAV2/CVC2/CVV2/CID (security code)
▪ Expiration date	▪ PINs
▪ Service Code	

## Locate all PCI data in each database

### **Crawl through each enterprise database to identify PCI data**

- Use the results from step one to check each database for PCI data
- Understand relationships across fields & systems to reveal PCI data
- Look for PCI data embedded within a field
- Review hundreds of tables and millions of rows



### **Classify PCI data as it is identified**

- Automatically find and categorize all instances of PCI data
- Continuously run classifier to ensure proper classification over time



### **Focus efforts on those databases which contain PCI data**

- Use limited resources to protect those databases at high risk

- ✓ **Satisfy Requirement #3:**
  - **Protect stored cardholder data**

## Pass critical information to Security Information & Event Manager

### Database activity monitoring with SIEM

- ✓DAM provides granular database monitoring and protection
- ✓DAM means low overhead; no reliance on native logging
- ✓DAM export alerts and key data to SIEM
- ✓SIEM provides forensics for DAM alerts

- ✓Satisfy Requirement #12 :
  - Maintain a policy that addresses information security for all personnel





Will purchasing Guardium make me PCI-DSS Compliant?

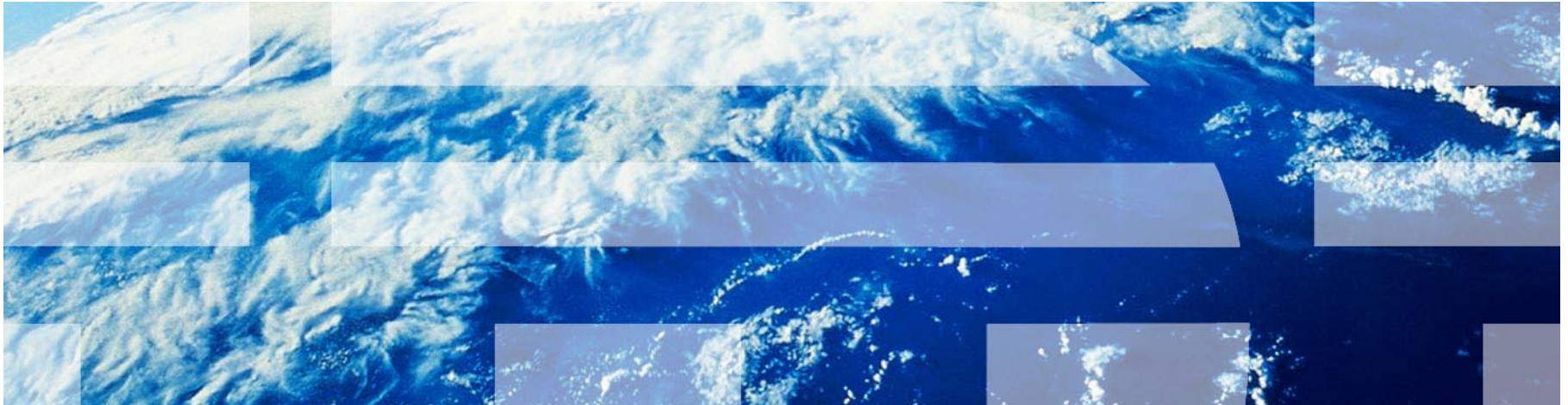
**NO.**

**BUT...**

With Guardium's tailored PCI-DSS Accelerator, including  
**150 PCI-centric precompiled reports and policies,**  
IBM can give you a kick-start on the **Journey** of becoming  
PCI-DSS compliant

# The Protection of Personal Information Act

***PoPI***



## What is PoPI?



**The Bill aims to protect the individual's right to data privacy and protection of personal information and seeks to balance this right against other rights, for example the right of access to information, including the needs of businesses to be able to process information and data for commercial ends.**

## What is PoPI?

### The Bill -

- gives effect to the constitutional right to privacy of personal information;
- requires all individuals, entities and particularly businesses, **to establish new methods of operating** with regard to the collection and/or dissemination of any personal information stored in any manner;
- requires businesses to review their arrangements with agencies and intermediaries;
- necessitates the amendment of all contracts to include consent provisions;
- requires businesses to implement **policies on privacy and information security**;
- and brings South Africa into line with international laws on data protection.

In summary, it seeks to achieve these goals by requiring that users of Personal Information comply with certain data protection principles which regulate how an individual's personal information may be used. Users are also required to notify a new body, the Information Protection Regulator, about their use of any individual's personal information.

## Enforcement and Penalties

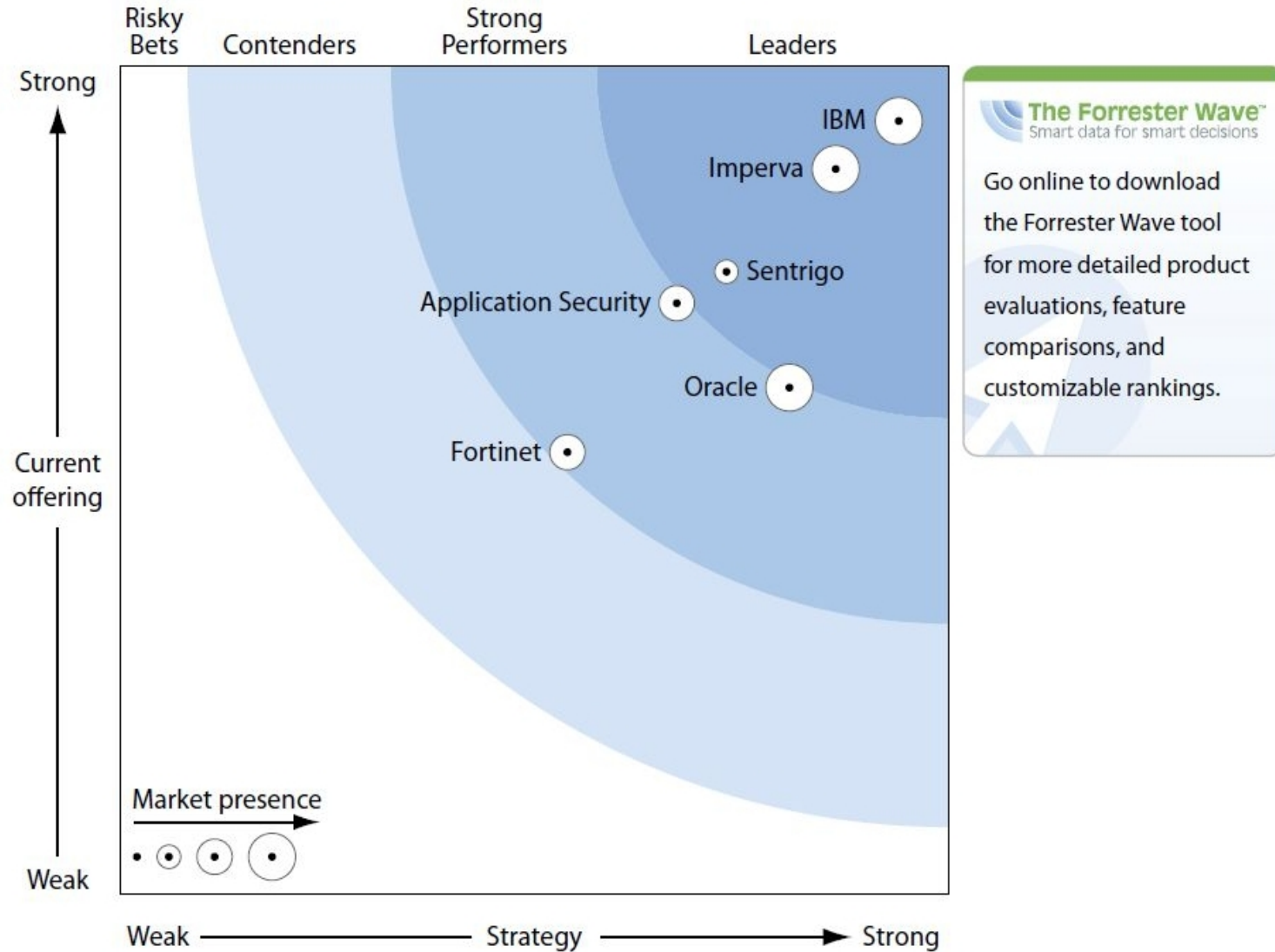
The Bill contains a complaints procedure whereby any person may lodge a complaint with the Regulator in certain circumstances, including for a breach of the Principles or the provisions relating to unsolicited communications, directories and automated decision-making. The Regulator has extensive powers of investigation including the right to apply to court for a warrant to enter and search premises. Data Subjects (or the Regulator on behalf of a Data Subject) may also bring **a claim for damages** in certain circumstances, **irrespective of whether there is intent or negligence involved**.

Contravention of any of the Principles is not, in itself a criminal offence. However the Regulator has the power to issue enforcement notices for certain breaches of the Bill and failure to comply with an enforcement notice is a criminal offence.

On conviction of an offence under the Bill, **a person is liable to a fine and/or up to 12 months imprisonment**, except if the offence relates to obstructing the Regulator, in which case the person is liable to a fine and/or up to 10 years imprisonment.



**Figure 2** Forrester Wave™: Database Auditing And Real-Time Protection, Q2 '11



# The Choice of Middle East & Africa



# The Choice of Financial Services (9 of the Top 10 Major Banks)





# The Choice of the Fortune 500

				JPMORGAN CHASE & CO.



# Questions



Thank  
YOU

The text "Thank YOU" is rendered in a large, 3D, light blue font. Each letter of the word "Thank" and the word "YOU" contains a different portrait of a person. The portraits are arranged in two rows: the top row for "Thank" and the bottom row for "YOU". The portraits include a man in a suit and tie, a woman in a green top, a man with a green face, a man with glasses, a man with a blue shirt, a man in a white lab coat, a man in an orange shirt, and a woman in a green top.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.



[ibm.com/security](http://ibm.com/security)

© **Copyright IBM Corporation 2012. All rights reserved.** The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.